

综合辅导：电子商务安全体系的发展与动态电子商务考试

PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/517/2021_2022__E7_BB_BC_E5_90_88_E8_BE_85_E5_c40_517187.htm 关键词：电子商务

(Electronic Commerce) 是在Internet开放的网络环境下，基于浏览器/服务器应用方式，实现消费者的网上购物、商户之间的网上交易和在线电子支付的一种新型的商业运营模式。Internet上的电子商务可以分为三个方面：信息服务、交易和支付。主要内容包括：电子商情广告；电子选购和交易、电子交易凭证的交换；电子支付与结算以及售后的网上服务等。主要交易类型有企业与个人的交易(B to C方式)和企业之间的交易(B to B方式)两种。参与电子商务的实体一般来讲有四类：顾客(个人消费者或企业集团)、商户(包括销售商、制造商、储运商)、银行(包括发卡行、收单行)及认证中心。电子商务是Internet爆炸式发展的直接产物，是网络技术应用的全新发展方向。Internet本身所具有的开放性、全球性、低成本、高效率的特点，也成为电子商务的内在特征，并使得电子商务大大超越了作为一种新的贸易形式所具有的价值，它不仅会改变企业本身的生产、经营、管理活动，而且将影响到整个社会的经济运行与结构。现阶段推动电子商务面临的最大问题是如何保障电子商务过程中的安全性，交易的安全是网上贸易的基础和保障，同时也是电子商务技术的难点。近年来，国际上已实施和制定了一系列的方法来解决网上交易的安全性问题。

1、电子商务的安全控制要求概述

电子商务发展的核心和关键问题是交易的安全性。由于Internet本身的开放性，使网上交易面临了种种危险，也由此提出了相应的

安全控制要求。 1.1信息保密性 交易中的商务信息有保密的要求。如信用卡的帐号和用户名被人知悉，就可能被盗用，订货和付款的信息被竞争对手获悉，就可能丧失商机。因此在电子商务的信息传播中一般均有加密的要求。 1.2交易者身份的确定性 网上交易的双方很可能素昧平生，相隔千里。要使交易成功，首先要能确认对方的身份，对商家而言要考虑客户端不能是骗子，而客户也会担心网上的商店不是一个弄虚作假的黑店。因此能方便而可靠地确认对方身份是交易的前提。 1.3不可否认性 由于商情的千变万化，交易一旦达成是不能被否认的。否则必然会损害一方的利益。 1.4不可修改性 交易的文件是不可被修改的，如其能改动文件内容，那么交易本身便是不可靠的，客户或商家可能会因此而蒙受损失。因此电子交易文件也要能做到不可修改，以保障交易的严肃和公正。

2、电子商务安全交易的有关标准和实施方法

2.1安全交易的雏形

在电子商务实施初期，曾采用过一些简易的安全措施，这些措施包括：

- (1) 部分告知(Partial Order)：即在网上传输交易中将最关键的数据如信用卡号码及成交数额等略去，然后再用电话告之，以防泄密。
- (2) 另行确认(Order Confirmation)：即当在网上传输交易信息之后，再用电子邮件对交易作确认，才认为有效。
- (3) 在线服务(Online Service)：为了保证信息传输的安全，用企业提供的内部网来提供联机服务。

以上所述的种种方法，均有一定的局限性，且操作麻烦，不能实现真正的安全可靠性。

2.2安全交易标准的制定

近年来，IT业界与金融行业一起，推出不少更有效的安全交易标准。主要有：

- (1) 安全超文本传输协议(S-HTTP)：依靠密钥对的加密，保障Web站点间的交易信息传输的安全性

。(2) 安全套接层协议 (SSL协议 : Secure Socket Layer)是由网景 (Netscape) 公司推出的一种安全通信协议, 是对计算机之间整个会话进行加密的协议, 提供了加密、认证服务和报文完整性。它能够对信用卡和个人信息提供较强的保护。SSL被用于Netscape Communicator和Microsoft IE浏览器, 用以完成需要的安全交易操作。在SSL中, 采用了公开密钥和私有密钥两种加密方法。(3) 安全交易技术协议(STT : Secure Transaction Technology) : 由Microsoft公司提出, STT将认证和解密在浏览器中分离开, 用以提高安全控制能力。Microsoft将在Internet Explorer中采用这一技术。(4) 安全电子交易协议 (SET : Secure Electronic Transaction) : SET协议是由VISA和MasterCard两大信用卡公司于1997年5月联合推出的规范。SET主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的, 以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份、以及可操作性。SET中的核心技术主要有公开密匙加密、电子数字签名、电子信封、电子安全证书等。目前公布的SET正式文本涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整及数字认证、数字签名等。这一标准被公认为全球网际网络的标准, 其交易形态将成为未来“电子商务”的规范。支付系统是电子商务的关键, 但支持支付系统的关键技术的未来走向尚未确定。安全套接层 (SSL) 和安全电子交易 (SET) 是两种重要的通信协议, 每一种都提供了通过Internet进行支付的手段。但是, 两者之中谁将领导未来呢? SET将立刻替换SSL吗? SET会因其复杂性而消亡吗? SSL真的能完全满足电子商务的需要吗? 我们可以从以下几点对比作管中一窥: SSL提供了两台机

器间的安全连接。支付系统经常通过在SSL连接上传输信用卡卡号的方式来构建，在线银行和其他金融系统也常常构建在SSL之上。虽然基于SSL的信用卡支付方式促进了电子商务的发展，但如果想要电子商务得以成功地广泛开展的话，必须采用更先进的支付系统。SSL被广泛应用的原因在于它被大部分Web浏览器和Web服务器所内置，比较容易被应用。SET和SSL除了都采用RSA公钥算法以外，二者在其他技术方面没有任何相似之处。而RSA在二者中也被用来实现不同的安全目标。SET是一种基于消息流的协议，它主要由MasterCard和Visa以及其他一些业界主流厂商设计发布，用来保证公共网络上银行卡支付交易的安全性。SET已经在国际上被大量实验性地使用并经受了考验，但大多数在Internet上购的消费者并没有真正使用SET。SET是一个非常复杂的协议，因为它非常详细而准确地反映了卡交易各方之间存在的各种关系。SET还定义了加密信息的格式和完成一笔卡支付交易过程中各方传输信息的规则。事实上，SET远远不止是一个技术方面的协议，它还说明了每一方所持有的数字证书的合法含义，希望得到数字证书以及响应信息的各方应有的动作，与一笔交易紧密相关的责任分担。F8F8" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com